METHOD AND SYSTEM FOR SECURE DELIVERY AND PRINTING OF DOCUMENTS

Field of the Invention

The invention disclosed herein relates generally to messaging technology, and more particularly to a system and method for providing secure, on-demand printing of documents delivered to a printing device.

Related Applications

This application is related to U.S. Applications Serial No. 09/707,561, filed November 7, 2000; Serial No. 09/727,893, filed November 30, 2000; Serial No. 09/728,237, filed November 30, 2000; Serial No. (Attorney Docket No. F-262), filed contemporaneously hereto; and Serial No. (Attorney Docket No. F-264), filed contemporaneously hereto; each assigned to the assignee of the present invention.

Background of the Invention

In today's rapidly paced society, professional and personal demands on messaging technologies, such as voice mail, e-mail, facsimile and pagers, have greatly increased. The development of this technology, in turn, has increased demands on mobile people who rely on these messaging devices for a variety of business and social communications. Specifically, these expectations have forced the mobile professional to demand the ability to receive messages regardless of time, location, or availability of messaging devices. According to a recent study by Pitney Bowes Inc. of Stamford, Connecticut, a typical business professional receives 169 messages a day. Many of these messages are delivered using some form of electronic and mobile communication such as cellular telephones, facsimiles, analog/digital telephone, pagers, e-mail transmission, and personal data assistants. These messages help determine the mobile professional's daily plans, keep him/her in contact with his/her community and enable him/her to accomplish his/her professional and personal goals.

Users, recognizing the capabilities of these devices, have relied on these devices such that they have become nearly indispensable tools for many businesses and individual consumers. Specifically recognized as invaluable are the inherent capabilities of a facsimile as an effective means of quickly and efficiently transmitting many types of documents from one known and specified location to another known and specified location. Facsimile machines are indispensable global tools, because they are used throughout the world and are accessible by and compatible with any other facsimile in the world. In addition, the use of facsimile machines has significantly improved the speed of transmittal of documents as compared to the sending of such a document through the postal services and/or various other express courier services, which, in general, require overnight delivery. Furthermore, facsimile machines have eased the travel burden on mobile professionals by eliminating the total number of printed documents they must carry to offsite meetings. With the aid of facsimile machines, any forgotten necessary documents may be retrieved by a simple facsimile.

In another messaging scenario, an individual may desire to print a hard copy of a document, an e-mail message or attachments to an e-mail message. In typical document messaging systems, a user desiring to print a document or message must be physically connected to a local printer or networked to a shared printer to print the document or message.

There are problems, however, with conventional document messaging systems. For example, a person desiring to print a document or message, or receive a facsimile of a document or message, must know the location of the device, and in the case of a facsimile, the facsimile number where a message may be received. If the message is a confidential communication, the user will desire to be present at the precise time the document or message is printed to claim the printed document or message before others see it. Otherwise, if the receiving facsimile machine or printer is in a public location, there is a risk that the message will be printed and left in an accessible location before the intended recipient gets there. Thus, if the intended recipient is not physically present at the facsimile machine or printer when the printing occurs, the intended recipient may never receive the message, and/or any confidentiality may be broken.

Similarly, if a shared network printer is being used to print a document or a message, there is a risk that the document or message will be printed and left in an accessible location before the user gets there to retrieve the printed document or message. Accordingly, any confidentiality may not be maintained.

Thus, there exists a need for a messaging system that can provide secure, on-demand printing of documents or messages delivered to a printing device, thereby ensuring receipt by the intended recipient and ensuring confidentiality of the contents of the document or message.

Summary of the Invention

The present invention alleviates the problems associated with the prior art and provides secure, on-demand printing of documents, messages and the like delivered to a printing device, such as, for example, a facsimile machine, printer or copier.

In accordance with the present invention, a user logs onto a document delivery system using a mobile device and selects a document, message or the like stored on a server to be printed along with a destination printing device for performing the printing. The document server encrypts the document to be delivered to the printing destination and creates a key. The key is sent to the mobile device. The document server sends the document to the destination printing device which stores the encrypted document. When the user is physically at the destination printing device, a connection is established between the mobile device and the destination printing device. The mobile device identifies to the printing device the document to be printed and sends the key to the printing device. The printing device uses the key to decrypt the document and then prints the document. Accordingly, the document will not be printed until the user is present at the printing device to retrieve the document as soon as it is printed.

According to another aspect of the present invention, if the document is not printed at the destination printing device within a predetermined period of time, it will be deleted from the destination printing device.

According to another aspect of the present invention, a selected document is encrypted and sent from the document server to the mobile device along with the key. When the user is physically at the destination printing device, a connection is established between the mobile device and the destination printing device, and the encrypted document and key are sent from the mobile device to the destination printing device. The printing device uses the key to decrypt the document and then prints the document. Accordingly, the document will not be printed until the user is present at the printing device to retrieve the document as soon as it is printed.

Description of the Drawings

The above and other objects and advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

FIG. 1 is a block diagram of a messaging system according to the present invention;

FIGS. 2A and 2B illustrate in flow diagram form a process flow of the messaging system according to an embodiment of the present invention;

FIG. 3 illustrates in flow diagram form a process flow of the messaging system according to another embodiment of the present invention; and

FIGS. 4A and 4B illustrate in flow diagram form a process flow of the messaging system according to another embodiment of the present invention.

Detailed Description of the Present Invention

In describing the present invention, reference is made to the drawings, wherein there is seen in Fig. 1 a system 10 for secure delivery and printing of documents according to the present invention. The term document, as used herein, refers to any type of document, message (e-mail, voicemail, textual, or any other message format), attachment to a message, or the like that is already in or

may be converted to electronic form and electronically transmitted. The system 10 includes a data center 12 that provides a document repository for a plurality of users. Thus, for example, a document 14 intended for a specified recipient is sent to data center 12 via communication link 16 and stored in data center 12. Each registered user of data center 12 is provided with a designated location for storage of documents intended for that user, such as, for example, a dedicated "In Box" similar to that found on conventional e-mail systems. While Fig. 1 illustrates document 14 being sent directly to data center 12, it should be understood the document 14 may first be sent to a specified recipient's default destination, such as, for example, an e-mail address, facsimile machine, or voice system, which then routes the document to data center 12.

System 10 also includes one or more mobile devices, such as mobile device 20, associated with each registered user of the system 10. Mobile device 20 may be a personal data assistant (PDA), pager, cell phone, laptop computer, or any other mobile wireless device typically carried by a user. Mobile device 20 is used to log into the data center 12 via a communication link 24 to determine if any documents 14 are presently stored in that user's in-box and to retrieve any stored documents as will be described below. Communication link 24 is preferably a wireless communication. Alternatively, data center 12, after receiving a new document 14, can identify the intended recipient and send a notification of receipt of document 14 to the recipient via any one of the mobile devices associated with the user, such as, for example, mobile device 20. Accordingly, a user will be notified upon receipt of a new document 14 and will not have to log into the data center 12 to determine if any new documents have been received and stored by the data center 12.

If a user wishes to print a document 14 stored in data center 20, the user selects an available destination printing device 22. Printing device 22 may be, for example, a facsimile machine, printer, photocopier or the like. The user establishes a communication link 26 between the mobile device 20 and printing device 22 for the exchange of information necessary for mobile device 20 to initiate the process of printing a document 14 using printing device 22. Communication link 26 can be either a wired link or a wireless link, such as, for example, an infrared or radio

frequency link. A wireless link can utilize ad-hoc, spontaneous networking technology such as, for example, Bluetooth or IEEE 802.11. Alternatively, a wireless link could also be a manual link, i.e., information can simply be input by the user directly to the mobile device 20 via a keypad or the like. Such information may include, for example, an address of the destination printing device 22, the telephone number of the printing device 22, and the types of encryption that the printing device 22 supports. Alternatively, the address or telephone number of previously used devices and types of encryption supported can be stored in mobile device 20 or data center 12 and retrieved from mobile device 20 by the user.

Once the mobile device 20 has the information necessary for initiating a print of a document 14, either by obtaining the information directly from printing device 22, manually inputting the information into mobile device 20, or recalling the information from a memory in mobile device 20 or data center 12, mobile device 20 will log into the data center 12 via communication link 24 and transmit the printing device 22 information to the data center 12. The user then selects a document 14 or group of documents he desires to retrieve and have printed. For example, a user may request two e-mail messages and one or more attachments to one of the e-mail messages to be printed, or an e-mail message and a text document. Data center 12 will encrypt the document(s) 14 and create a key for decrypting the document(s) 14. Any well known data encryption and decryption techniques may be used, such as those which use public and private key management. Optionally, data center 12 can establish a communication link 28 with the printing device 22 to interrogate printing device 22 as to the types of encryption supported by printing device 22 if this information is not known. The encrypted document(s) 14 are then sent from data center 12 to the destination printing device 22 via communication link 28 in accordance with the information provided by mobile device 20. The key created by data center 12 is sent to mobile device 20 via communication link 24, along with an identifier to identify the document(s) 14 as described below.

Printing device 22 will store the encrypted document(s) 14 upon receipt from data center 12. When the user is present at printing device 22, communication link 26 is established (if not previously established or re-established if the previous communication has been disrupted) between mobile device 20 and printing device

22. Communication link 26 can either be initiated by the user via mobile device 20 or be initiated spontaneously when mobile device 20 and printing device 22 are within a certain range of each other. Mobile device 20 identifies the desired document(s) 14 to be printed to printing device 22 and passes the associated key created by data center 12 to printing device 22 via communication link 26. Alternatively, as noted above, communication link 26 could be a wireless manual link, i.e., the identification of the desired document(s) 14 associated key could be manually input to printing device 22 via a keyboard or the like. The document(s) 14 to be printed can be identified by a header attached to the encrypted document(s) 14, by an extension attached to the encrypted document(s) 14, or any other manner as is known in the art. Printing device 22, upon receipt of the document(s) 14 identifier and associated key, will decrypt the document(s) 14 using the associated key and print the decrypted document(s) 14. Alternatively, once the printing device 22 has decrypted the document(s) 14, instead of automatically printing the document(s) 14 when the communication link 26 is established and the document(s) 14 identifier and key are transmitted, printing of the document(s) 14 could be under control of the user via a menu selection or the like displayed on a user interface of mobile device 20 or on the printing device 22.

Thus, according to the present invention, the printing of the document(s) 14 is not performed until the intended recipient is actually present at the printing device 22, thereby ensuring security of the contents of the document(s) 14 and receipt only by the intended recipient. A user can therefore schedule a delivery of the document(s) 14 to the printing device 22 and does not need to remain at the location of printing device 22 until the delivery and printing has been completed. Instead, the user can return at a later, more convenient time and complete the printing of the document(s) 14, without compromising the confidentiality of the document(s) 14.

As an added security feature, once the document(s) 14 have been printed, printing device 22 can optionally notify the data center 12 that printing has occurred and data center 12 can then notify mobile device 20 or any one of the other mobile devices associated with the user. Mobile device 20 can then provide an alert to the user that the document(s) 14 have been printed. Alternatively, printing device 22

can directly notify mobile device 20 or any one or more of the mobile devices associated with the user that printing has been completed.

Furthermore, if the destination printing device 22 does not receive the document(s) 14 identifier and associated key within a predetermined time period after receipt of the encrypted document(s) 14, the printing device 22 can remove the encrypted document(s) 14 from its memory, thereby increasing security of the document(s) 14 by preventing any unauthorized party from retrieving the document(s) 14 and attempting to decrypt and print them.

Figs. 2A and 2B illustrate in flow diagram form a process flow of the messaging system 10 according to one embodiment of the present invention. In step 50, one or more documents 14 are maintained in data center 12. When a user desires to print a document or group of documents, in step 52 it is determined if information, such as, for example, the address or telephone number, of the destination printing device 22 is known. If this information is not known, then in step 54 a communication is established between mobile device 20 and destination printing device 22, and in step 56 the information is sent from the printing device 22 to the mobile device 20. Once this information has been received in step 56 or if in step 52 the information is known, then in step 58 a communication is established between the mobile device 20 and data center 12. In step 60, the destination printing device 22 information is sent to the data center 12, or, if the destination printing device information is already stored in data center 12, the desired destination printing device 22 is selected. In step 62, a document 14 or group of documents are selected for printing via the communication between the mobile device 20 and data center 12. In step 64, the selected document(s) 14 are encrypted and a key is created by data center 12. In step 66, the encrypted document(s) are sent to the destination printing device 22, using the information obtained in step 60, and stored in destination printing device 22. In step 68 the key created by data center 12 is sent to the mobile device 20.

Referring now to Fig. 2B, in step 80 a communication is established (if not previously established or re-established if the previous communication has been disrupted) between the mobile device 20 and destination printing device 22. In step 82, the document(s) 14 identifier and key are sent from the mobile device 20 to the

destination printing device 22. In step 84, the printing device 22, using the document identifier and associated key, decrypts the document(s) 14 and in step 86 prints the decrypted document(s) 14. Optionally, in step 88, the printing device 22 can send confirmation of completion of printing of document(s) 14 to data center 12, mobile device 20, any one of the mobile devices associated with the user, or any combination of the above.

In accordance with another embodiment of the present invention, mobile device 20 will log into the data center 12 via communication link 24 and the user selects a document 14 or group of documents he desires to have printed. Data center 12 will encrypt the document(s) 14 and create a key for decrypting the document(s) 14. The encrypted document(s) 14 are then sent from data center 12 to the mobile device 20 along with the associated key. When the user is present at printing device 22, communication link 26 is established between mobile device 20 and printing device 22. Communication link 26 can either be initiated by the user via mobile device 20 or be initiated spontaneously when mobile device 20 and printing device 22 are within a certain range of each other. Mobile device 20 sends the encrypted document(s) 14 and the associated key created by data center 12 to printing device 22 via communication link 26. Printing device 22, upon receipt of the document(s) 14 and associated key, will decrypt the document(s) 14 using the associated key and print the decrypted document(s) 14 similarly as described above.

The operation of this embodiment is illustrated in the process flow diagram of Fig. 3. In step 50, one or more documents 14 are maintained in data center 12. When a user desires to print a document or group of documents, in step 100 a communication is established between the mobile device 20 and data center 12. In step 102, a document 14 or group of documents are selected for printing via the communication link 24 between the mobile device 20 and data center 12. In step 104, the selected document(s) 14 are encrypted and a key is created by data center 12. In step 106, the encrypted document(s) and key are sent to the mobile device 20. In step 108 a communication link 26 is established between the mobile device 20 and a destination printing device 22. In step 110, the encrypted document(s) 14 and key are sent from the mobile device 20 to the destination

printing device 22. In step 112, the printing device 22, using the key, decrypts the document(s) 14 and in step 114 prints the decrypted document(s) 14. Optionally, in step 116, the printing device 22 can send confirmation of completion of printing of document(s) 14 to data center 12, mobile device 20, any one of the mobile devices associated with the user, or any combination of the above.

In accordance with another embodiment of the present invention, if the printing device 22 is a networked device along with data center 12, then instead of sending a document(s) 14 identifier to mobile device 20, a pointer can be provided from data center 12 to mobile device 20 that points to the location of the document(s) 14 in the network. The pointer would then be provided from the mobile device to the printing device 22 along with the key used to encrypt the document(s) 14. Alternatively, the pointer and key could be manually input by the user to printing device 22. Alternatively, data center 12 could provide the pointer directly to the printing device 22. Printing device 22 would retrieve the document(s) 14 from the location in the network specified by the pointer and use the key to decrypt the document(s) 14 for printing. Thus, for example, if printing device 22 is a shared network printer, the document(s) 14 will not actually be printed until the user's mobile device 20 has established contact with the printing device 22.

Figs. 4A and 4B illustrate in flow diagram form a process flow of the messaging system 10 in which the destination printing device 22 is a networked device with data center 12. In step 50, one or more documents 14 are maintained in data center 12. When a user desires to print a document or group of documents, in step 52 it is determined if information, such as, for example, the address of the destination printing device 22 in the network, is known. If this information is not known, then in step 54 a communication is established between mobile device 20 and destination printing device 22, and in step 56 the information is sent from the printing device 22 to the mobile device 20. Once this information has been received in step 56 or if in step 52 the information is known, then in step 58 a communication is established between the mobile device 20 and data center 12. In step 60, the destination printing device 22 information is sent to the data center 12 or, if the destination printing device information is already stored in data center 12, the desired destination printing device 22 is selected. In step 62, a document 14 or

group of documents are selected for printing via the communication between the mobile device 20 and data center 12, or alternatively, selection of the document(s) 14 can be done by any device coupled to the network. In step 200, the selected document(s) 14 are encrypted and stored on the network and a key is created by data center 12. In step 202, a pointer indicating where the encrypted document(s) 14 are stored on the network is sent to the mobile device 20. Alternatively, the pointer could be sent directly to the destination printing device 22 along with a document identifier, using the information obtained in step 60. In step 204 the key created by data center 12 is sent to the mobile device 20.

Referring now to Fig. 4B, in step 210 a communication is established (if not previously established or re-established if the previous communication has been disrupted) between the mobile device 20 and destination printing device 22. In step 212, the pointer indicating where the encrypted document(s) 14 are stored on the network and key are sent from the mobile device 20 to the destination printing device 22 or input to the destination device 22. Alternatively, if the pointer was sent directly to the destination printing device 22, the key and document identifier which identifies the pointer are sent from the mobile device 20 to the destination printing device 22. In step 214, the printing device 22, using the pointer, retrieves the encrypted document(s) 14 from the network and decrypts the document(s) 14 using the associated key. In step 216, the printing device 22 prints the decrypted document(s) 14. Optionally, in step 218, the printing device 22 can send confirmation of completion of printing of document(s) 14 to data center 12, mobile device 20, any one of the mobile devices associated with the user, or any combination of the above.

Thus, according to the present invention, secure, on-demand printing of documents to a facsimile machine or networked printing device is provided, thereby ensuring receipt of the documents only by the intended recipient to maintain confidentiality of the document.

It should be noted that the order of the steps described in the above embodiments need not be as stated. For example, the selection of the documents to be printed could be performed before the destination printing device is selected and identified.

While preferred embodiments of the invention have been described and illustrated above, it should be understood that these are exemplary of the invention and are not to be considered as limiting. Additions, deletions, substitutions, and other modifications can be made without departing from the spirit or scope of the present invention. Accordingly, the invention is not to be considered as limited by the foregoing description but is only limited by the scope of the appended claims.